FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER	
GIC-574	
U S APPLICATION NO (If known, see 37 CFR 1 5	
09/937790	
INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE
PCT/US00/09800	12 April 2000
PRIORITY DATE CLAIMED	
04 May 1999	

TITLE OF INVENTION METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES

APPLICANT(S) FOR DO/EO/US
R. Safadi, et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [X] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [ ] has been communicated by the International Bureau.
   c. [X] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [ ] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [X] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
    Please include assignee information when this application is published.
13. [X] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [X] Other items or information:
    (a) Patent Application Data Entry Form - 1 sheet
    (b) Patent application specification including claims and abstract - 28 pages (incorporates amendments made on April 19, 2001 and indicated on the Annexes to the International Preliminary Examination Report dated 8/2/01)
    (c) Three (3) sheets of formal drawings, together with transmittal letter
    (d) Express Mail Certificate

U.S. APPLICATION NO (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937790	PCT/US00/09800	GIC-574

21. [X] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 690.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ ---	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	42 - 20 =	22	x **$18.00**	$ 396.00	
Independent claims	2 - 3 =	0	x **$80.00**	$ 0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$ ---	
TOTAL OF ABOVE CALCULATIONS =				$ 1086.00	
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.			+	$ ---	
SUBTOTAL =				$ 1086.00	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ ---	
TOTAL NATIONAL FEE =				$ 1086.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$ 1126.00	
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $ 1126.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0625 . A duplicate copy of this sheet is enclosed.

d. [ ] Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO.

Barry R. Lipsitz
Law Offices of Barry R. Lipsitz
755 Main Street, Building No. 8
Monroe, CT 06468
(203) 459-0200

Date: 28 September 2001

SIGNATURE

Barry R. Lipsitz
NAME

28,637
REGISTRATION NUMBER

Express Mail No.: EL 827 617 155 US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
R. SAFADI, et al.)
)
Filed: Herewith)
)
Title: **METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES**)

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail (No. EL 827 617 155 US) in an envelope addressed to: BOX PCT , Commissioner for Patents, Washington, D.C. 20231 on:

By: Cathy Dunne September 28, 2001
Cathy Dunne

BOX PCT
Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Dear Sir:

Prior to examination of the above-referenced U.S. patent application, please amend the application as follows:

IN THE SPECIFICATION:

Please amend the specification by inserting before the first line the paragraph:

"This application claims the benefit of international application number PCT/US00/09800 filed April 12, 2000. The

international application was published under PCT Article 21(2) in the English language."

REMARKS

Applicants are herewith entering the national stage in the United States under 35 U.S.C. 371 of international application no. PCT/US00/09800. This Preliminary Amendment amends the specification to indicate that the corresponding international application PCT/US00/09800 was published in the English language under PCT Article 21(2).

Entry of this Amendment is respectfully requested.

Respectfully submitted,

Barry R. Lipsitz
Attorney for Applicant(s)
Registration No. 28,637
755 Main Street
Monroe, CT 06468
(203) 459-0200

Date: September 28, 2001
ATTORNEY DOCKET NO.: GIC-574

3/prts

METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES

This application claims the benefit of U.S. provisional patent application no.60/132,366 filed May 4, 1999.

BACKGROUND OF THE INVENTION

The present invention relates to the communication of information services over a communication network, and more particularly to providing access control for signals containing audiovisual content and services, such as on-demand television programming. In order to render subscription programming services and the like commercially viable, systems must be provided for preventing non-paying individuals from obtaining the services. Such "access control" systems can take various forms, but generally include some type of modification (e.g., scrambling) or encryption of the signals that carry the services. Only authorized subscribers have access to the elements (e.g., cryptographic keys) necessary to satisfactorily receive the signals.

Current techniques for decryption of signals such as on-demand services may be based on real time hardware based encryption solutions or based on pre-encryption methods. Some configurations allow for

cost effective real time encryption at the transport level but are not as effective at a service level. Such problems, together with the following additional factors, require a new solution that provides a reliable and cost-effective means for access control of on-demand services:

1. Current real-time encryption does not meet the cost model for on-demand services, in that it is expensive to implement.
2. In some configurations real time encryption requires too much real-estate at service provider sites (currently, for example, various video-on-demand (VOD) vendors are consolidating their servers and signal modulators (e.g., QAM modulators) in space efficient packaging which bypasses a real-time encryption stage).
3. Pre-encryption is inherently not as secure as real-time encryption. At the same time, on-demand content security requirements are less stringent than those of broadcast content. For example, there is no *a priori* knowledge of when certain content will be requested in the on-demand case. In the broadcast case, the content is always being sent and the schedules are known ahead of time.
4. MPAA (Motion Picture Association of America) has issues with clear (i.e., unencrypted)

content, such as movies, and expects such content to be protected.

5. Entitlement control should be upgradeable without impacting content providers or server vendors. Stronger solutions should be able to be incorporated gradually as the need dictates.
6. Secure content delivery of MPEG-2 (Motion Picture Experts Group) using Internet Protocol (IP) for point to point on demand services or multicast services must be facilitated.
7. Transport independent entitlement control (e.g., MPEG-2 or IP) must be provided.

It would be advantageous to provide a method and apparatus for access control of on-demand services that addresses the above-noted issues. In particular, it would be advantageous to provide a content pre-encryption method that enables entitlement control to be effectively implemented independent of the transport protocol, e.g., MPEG-2 or IP.

It would be still further advantageous to provide such a capability that can be offered as a separate service to content providers, server vendors, and cable system operators. The present invention can be adapted for use with different

types of provider networks, e.g. satellite and Internet based networks.

The present invention provides a system having these and other advantages. In particular, the invention disclosed herein extends existing encryption capability, such as that provided by the Digicipher II (DCII) system available from General Instrument Corporation of Horsham, Pennsylvania, USA, the assignee of the present invention, to handle pre-encrypted content that is requested on demand by a viewer or is sent to a group of viewers. The method of the invention is also upgradeable to facilitate implementations of entitlement control algorithms that vary in sophistication as the need dictates. Additionally, the method is extensible to enable encryption control that is independent of the transport protocol used. Such protocols include, for example, MPEG-2 and Internet Protocol (IP).

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and apparatus are provided for access control of pre-encrypted on-demand content. In a simplified embodiment, the content is pre-encrypted by an encryption device controlled by a pre-encryption controller. The pre-encrypted content is forwarded from the encryption device to a server. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag to the user terminal and a second tag to the server. The first tag is associated with the second tag and the second tag acts as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller. The pre-encrypted content is communicated from the server to a user terminal via a first communication path.

An entitlement authorization associated with the encrypted content is communicated to a user terminal (e.g., a "client device" such as a set-top box) via a second communication path independent of said first communication path. Authorization to access the pre-encrypted content is determined based on said entitlement authorization and said first tag upon demand of said content by a user.

The user terminal may be a set-top box, a

digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

The pre-encryption controller acts to set up the encryption device for pre-encrypting the content. The set up of the encryption device is outside the scope of this invention. For background purposes, it will suffice to state that the pre-encryption controller, through bi-directional communication with the encryption device, configures the encryption device with appropriate parametric values and commands to enable the encryption device appropriately to encrypt the content.

In an alternate embodiment, the server is a main server (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal via a local distribution server. The pre-encryption controller is in communication with a local distribution controller (e.g., a head-end controller in a cable television implementation), which local distribution controller communicates the entitlement authorization to the user terminal.

In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

In one embodiment, the ODB and URH are both

forwarded to both the local distribution controller and the server from the pre-encryption controller. In an alternate embodiment, only the URH is forwarded to the main server and the ODB is communicated from the local distribution controller to the local distribution server.

In one embodiment the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB are stored as an attribute of the encrypted content.

The ODB may be processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server. This processing at the local distribution controller may include algorithmically modifying the ODB. Such reprocessing of the ODB at the local distribution controller provides an added level of security since the post-processing ODBs are no longer the same across multiple local distribution controllers.

The ODB itself may be coded in a manner that is not readily discernable by third parties. Alternatively, the ODB content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of security. In

this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors. In the on-demand case, the ODB itself may also be encrypted, using, for example, the recipient's public key.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

In a preferred embodiment, a client application (typically software residing in a user terminal such as a set-top box) then requests specific content from the server, such as a video on demand (VOD) movie or any other interactive content. The ODB is forwarded from a server application to the client application software that typically resides in a central processor (CPU) of the user terminal. After this set-up is completed, the server starts sending the pre-encrypted content to the user terminal. The ODB is then forwarded from the client application via an application program interface in the CPU to a kernel located in the user terminal. The ODB is then

processed in the user terminal in conjunction with the received entitlement authorization to determine whether to decrypt the received pre-encrypted content.

Processing may be provided by a secure processor located in the user terminal or a software task included in the user terminal CPU. The pre-encrypted content is received by the user terminal and decrypted when authorization is granted. Upon authorization, the content will be processed for display.

The pre-encrypted content may be received by the secure processor via a conventional receiver circuit. Alternatively, the pre-encrypted content may be received by the secure processor via direct memory access from device memory.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of the functional components of the flexible pre-encryption architecture of the invention;

Figure 2 is a block diagram of another embodiment of the functional components of the flexible pre-encryption architecture of the invention; and

Figure 3 is a block diagram of the relevant components of a user terminal in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 illustrates the main components of an on-demand content communication system in accordance with the present invention. In particular, a method and apparatus are provided for access control of pre-encrypted on-demand content. The video encoder and post encoding processors are not shown, since they are well known in the art. As will be appreciated by those skilled in the art, any type of post processing to be done on the content file/data stream is performed prior to encryption.

Referring to Figure 1, a pre-encryption controller 10 sets up an encryption device 14 for encryption of the content 15. A server 12 forwards the content file/stream to the encryption device 14 for encryption of the content prior to distribution ("pre-encryption"). The encryption device encrypts the content file and forwards the pre-encrypted content back to the main server 12.

The pre-encryption controller 10 acts to set up the encryption device 14 for pre-encrypting the content. The set up of the encryption device 14 is outside the scope of this invention. For background purposes, it will suffice to state that the pre-encryption controller 10, through bi-directional communication with the encryption device 14, configures the encryption device 14 with appropriate parametric values and commands to enable the

encryption device 14 appropriately to encrypt the content.

In one embodiment as shown in Figure 1, the pre-encrypted content is forwarded from the encryption device 14 to a server 12. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag and a second tag to the server 12 via line 17. The first tag is also provided to a user terminal 20 via line 19 or 21 depending upon the particular implementation, the first tag being associated with said second tag. The second tag acts as a reference to the pre-encrypted content and associated first tag, wherein the first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller 10. The pre-encrypted content is communicated from the server 12 to a user terminal 20 (e.g., a "client device" such as a set-top box) via a first communication path 21.

An entitlement authorization associated with the encrypted content is communicated to the user terminal 20 via a second communication path 19 independent of the first communication path. Authorization to access the pre-encrypted content is determined at the user terminal 20 based on said entitlement authorization and the first tag upon demand of the content by a user. Communication from the user terminal 20 back to the server 12 is provided on line 23.

The user terminal 20 may be a set-top box, a digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

In an alternate embodiment shown in Figure 2, the server is a main server 12' (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal 20 via lines 25 and 27 and a local distribution server 18. The main server 12' can distribute the encrypted content to various local distribution servers (at various service provider locations, e.g., head-ends). The pre-encryption controller 10 is in communication with a local distribution controller 16, which controls, e.g., a cable television system or the like in a well known manner (e.g., a head-end controller in a cable television implementation). The local distribution controller 16 communicates the entitlement authorization to the user terminal 20 via line 29.

In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

In one embodiment, the ODB and URH are both forwarded to both the local distribution controller 16 (via line 11) and the main server 12' (via line 13) from the pre-encryption controller 10. In an

alternate embodiment, only the URH is forwarded to the main server 12' and the ODB is communicated from the local distribution controller 16 to the local distribution server 18 via line 22.

Either the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB may be stored as an attribute of the encrypted content.

The ODB may be processed at the local distribution controller 16 to generate a modified, second ODB, which second ODB is forwarded from the local distribution controller 16 to the local distribution server 18. This processing at the local distribution controller 16 may include algorithmically modifying the ODB. This may be done as an offline process. Such reprocessing of the ODB at the local distribution controller 16 provides an added level of security since the post-processing ODBs are no longer the same across multiple local distribution controllers.

The system manufacturer specifies the ODB content and, for security reasons, the ODB itself may be coded in a manner that is not readily discernable by third parties. Alternatively, the ODB content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of

security. In the on-demand case, the ODB itself may also be encrypted (with an additional level of implementation complexity) using, for example, the recipient's public key. In the case of broadcast or multicast content, the ODB may be made available in advance since it is associated with the event or content to be viewed or received. Encryption of the ODB using the user's public key is extremely useful for the IP transport case where the system administrator has the option to make known what events are available when, e.g. via an Electronic Programming Guide (EPG). In this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors. In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user terminal 20 with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using the ODB.

Figure 3 depicts the processing that takes place at the user terminal 20. The client application 40 (typically residing in a user terminal 20 such as a set-top box) requests specific content from the server (either the server 12 of Figure 1 or local distribution server 18 of Figure 2), such as a video on demand (VOD) movie or any other interactive content. The server then sends the ODB to the client application device 40. After this set-up is completed, the server 18 starts sending the pre-encrypted content to the user terminal 20.

The client application 40 (e.g. software) running in the user terminal processor (CPU) 36 receives the ODB from a server application in the server 12 or local distribution server 18, as described in connection with Figures 1 and 2, and forwards it via an application program interface (API) 42 to the user terminal processor kernel 44. In the broadcast and multicast modes, the ODB may be made available ahead of time, before the actual broadcast or multicast event commences. In this case the ODB may be requested by and sent to the user by the local distribution controller (16). The ODB is then processed in the user terminal 20 in conjunction with the received entitlement authorization (as described in connection with Figures 1 and 2) to determine whether to decrypt the received pre-encrypted content.

Processing may be provided by a secure processor 32 located in the user terminal 20 or a software task included in the CPU 36. The pre-encrypted content is received by the user terminal 20 and decrypted when authorization is granted. Upon authorization, the content will be processed for display.

The pre-encrypted content may be received by the secure processor 32 via a conventional receiver circuit (i.e. receiver output of Figure 3). Alternatively, the pre-encrypted content may be received by the secure processor 32 via direct memory access from device memory 30. The decrypted output from the secure processor 32 is written back to memory 30 for further use by the CPU 36, or is forwarded to a demultiplexer/decoder 34 for further processing in a conventional manner.

It should now be appreciated that the present invention provides an improved method and apparatus for the delivery and access of pre-encrypted on-demand television services. In particular, the present invention provides a content pre-encryption method and apparatus that enables entitlement control to be effectively implemented independent of the transport protocol, e.g., MPEG-2 or Internet Protocol (IP), and to some extent independent of transmission mode (i.e., singlecast (e.g., on-demand), multicast, or broadcast). Additionally, the present invention provides encryption and access

control capability that can be offered as a separate service to content providers, server vendors, cable system operators, and/or Internet service providers, or the like. The present invention enables entitlement authorization that can vary in sophistication as deemed necessary without burdening the content providers or service vendors. In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

Although the invention has been described in connection with certain preferred embodiments, it should be appreciated that numerous adaptations and modifications may be made thereto without departing from the scope of the invention as set forth in the claims.

What is claimed is:

1. A method of providing access control for pre-encrypted on-demand content, comprising the steps of:

pre-encrypting the content;

forwarding the pre-encrypted content to a server;

providing a first tag to a user terminal, said first tag being associated with a second tag;

said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by a pre-encryption controller;

providing at least said second tag to said server;

communicating the pre-encrypted content from said server to said user terminal via a first communication path;

communicating an entitlement authorization associated with the pre-encrypted content to said user terminal via a second communication path independent of said first communication path; and

determining whether said user terminal is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

2. A method in accordance with claim 1, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

3. A method in accordance with claim 2, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

4. A method in accordance with claim 3, comprising the further step of forwarding the ODB and associated URH to the local distribution controller.

5. A method in accordance with claim 3, wherein only the URH is forwarded to the main server, further comprising the steps of:

communicating the ODB from the local distribution controller to the local distribution server.

6. A method in accordance with claim 5, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second

ODB is forwarded from the local distribution controller to the local distribution server.

7. A method in accordance with claim 3, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

8. A method in accordance with claim 3, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

9. A method in accordance with claim 3, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

10. A method in accordance with claim 3, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

11. A method in accordance with claim 3, further comprising the steps of:

forwarding the ODB from a server application via an application program interface in the user terminal to a kernel located in the user terminal;

processing the ODB in conjunction with the received entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content;

receiving the pre-encrypted content;

decrypting the pre-encrypted content when authorization is granted; and

processing the decrypted content for display.

12. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via a receiver circuit.

13. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via direct memory access from device memory.

14. A method in accordance with claim 3, wherein the ODB is coded in a manner that is not readily discernable by third parties.

15. A method in accordance with claim 3, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

16. A method in accordance with claim 3, wherein the ODB itself is encrypted.

17. A method in accordance with claim 16,

wherein the ODB is encrypted using the user's public key.

18. A method in accordance with claim 3, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

19. A method in accordance with claim 3, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

20. A method in accordance with claim 3, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

21. A method in accordance with claim 3, wherein the pre-encrypted content is accessed via the Internet.

22. An apparatus for providing access control for pre-encrypted on-demand content, comprising:

an encryption device for encrypting the content;

a server for receiving the pre-encrypted content from the encryption device;

a pre-encryption controller for generating a first tag and an associated second tag, said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first tag and second tag are unique to the pre-encrypted content and are tracked by the pre-encryption controller;

a user terminal for receiving entitlement

authorization associated with the pre-encrypted content;

said first tag being communicated to the user terminal and said second tag being communicated to the server;

wherein the user terminal determines whether it is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

23. An apparatus in accordance with claim 22, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

24. An apparatus in accordance with claim 23, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

25. An apparatus in accordance with claim 24, wherein the local distribution controller receives the ODB and associated URH from the pre-encryption controller.

26. An apparatus in accordance with claim 24, wherein:

the main server receives only the URH from the pre-encryption controller; and

the local distribution controller communicates the ODB to the local distribution server.

27. An apparatus in accordance with claim 26, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server.

28. An apparatus in accordance with claim 24, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

29. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

30. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

31. An apparatus in accordance with claim 24, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

32. An apparatus in accordance with claim 24, wherein the user terminal comprises:

a client application using a program interface for forwarding the ODB from the local distribution server to a kernel

said kernel receiving the ODB the application program interface and the entitlement authorization from the local distribution controller; and

a secure processor for receiving the ODB and entitlement authorization from the kernel and receiving the pre-encrypted content from the local distribution server, wherein the processor processes the ODB in conjunction with entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content.

33. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via a receiver circuit.

34. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via direct memory access from device memory.

35. An apparatus in accordance with claim 24, wherein the ODB is coded in a manner that is not readily discernable by third parties.

36. An apparatus in accordance with claim 24, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

37. An apparatus in accordance with claim 24, wherein the ODB itself is encrypted.

38. An apparatus in accordance with claim 37, wherein the ODB is encrypted using the user's public key.

39. An apparatus in accordance with claim 24, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

40. An apparatus in accordance with claim 24, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

41. An apparatus in accordance with claim 24, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

42. An apparatus in accordance with claim 24, wherein the pre-encrypted content is accessed via the Internet.

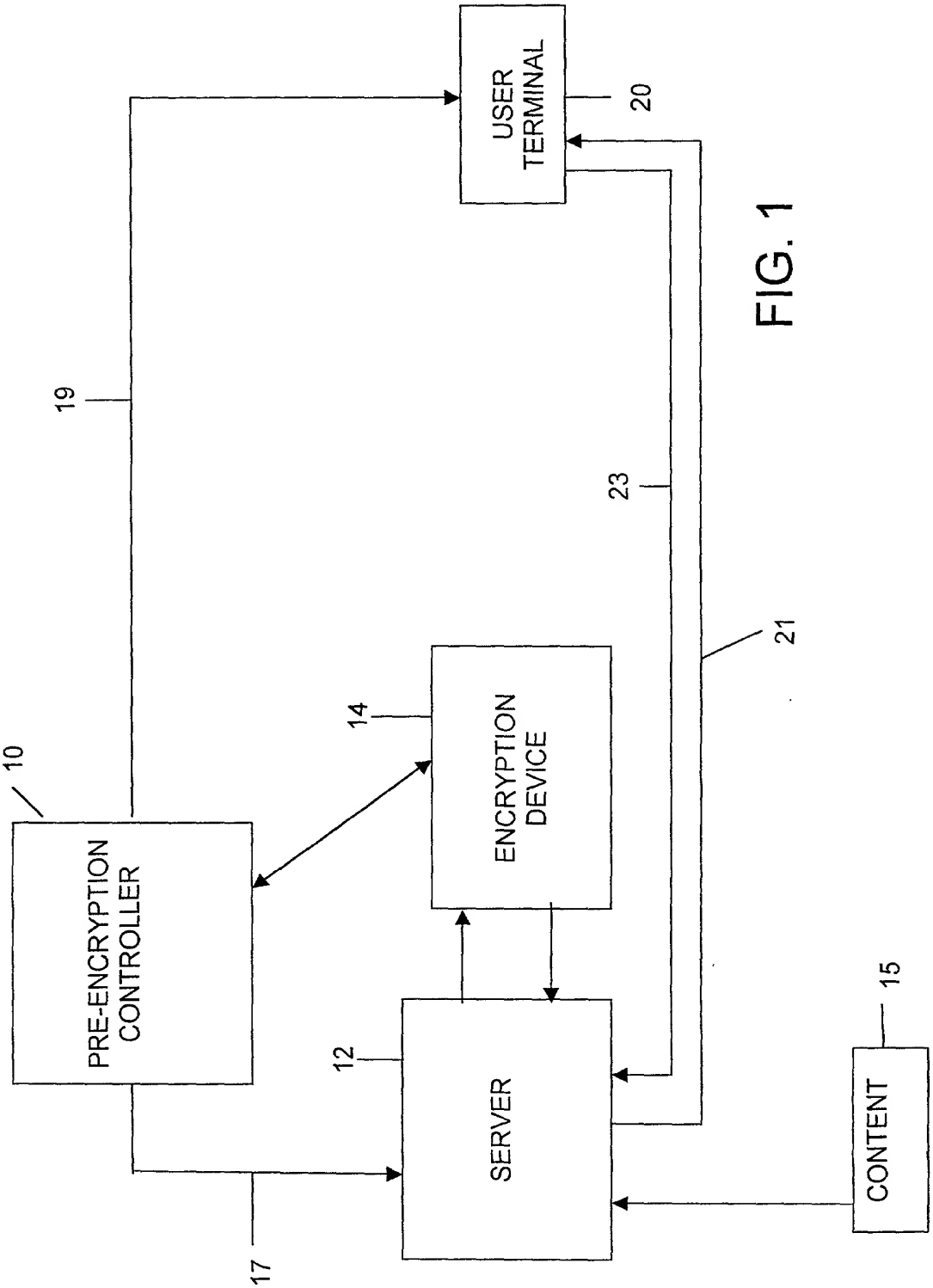

FIG. 1

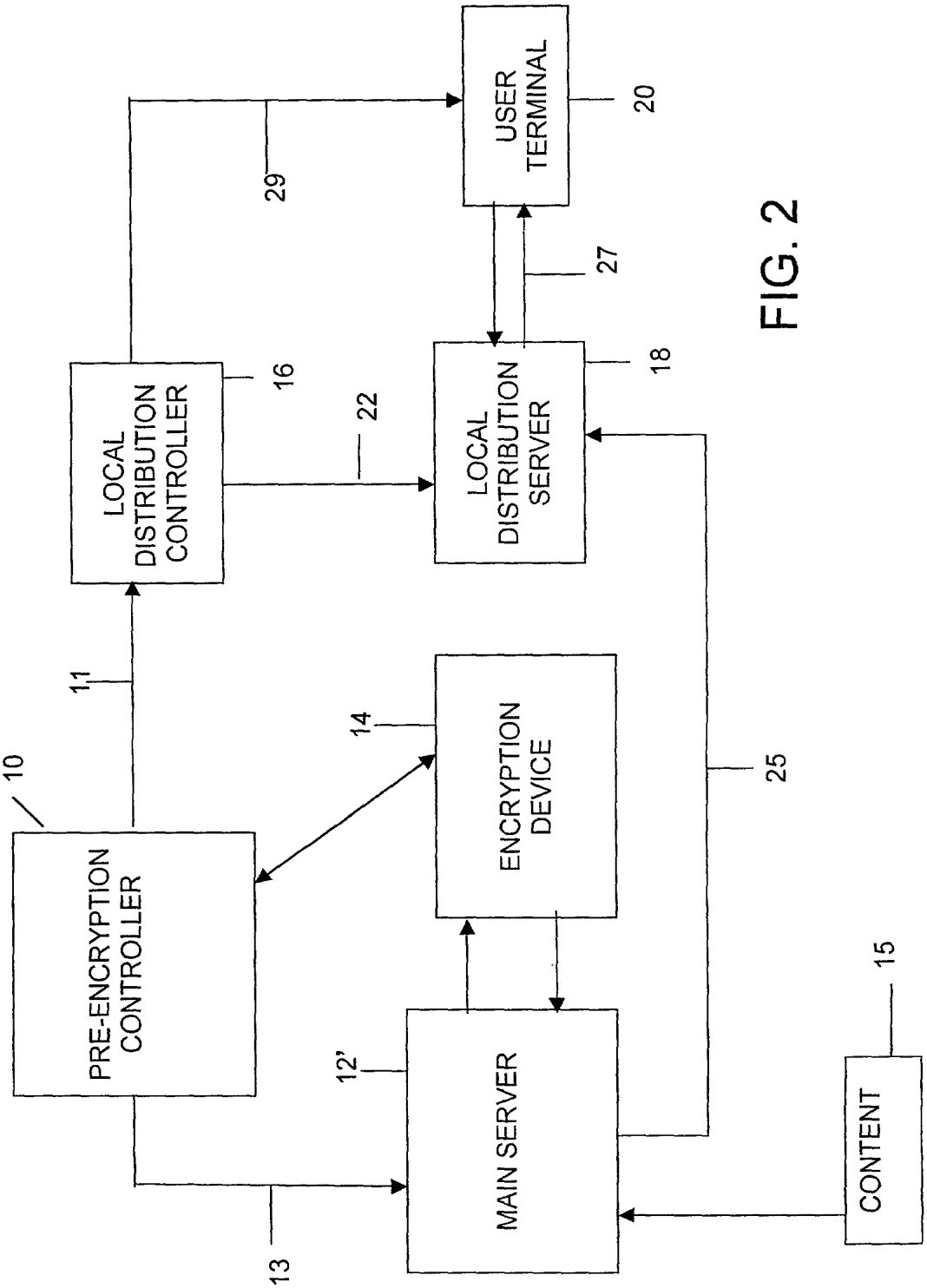

FIG. 2

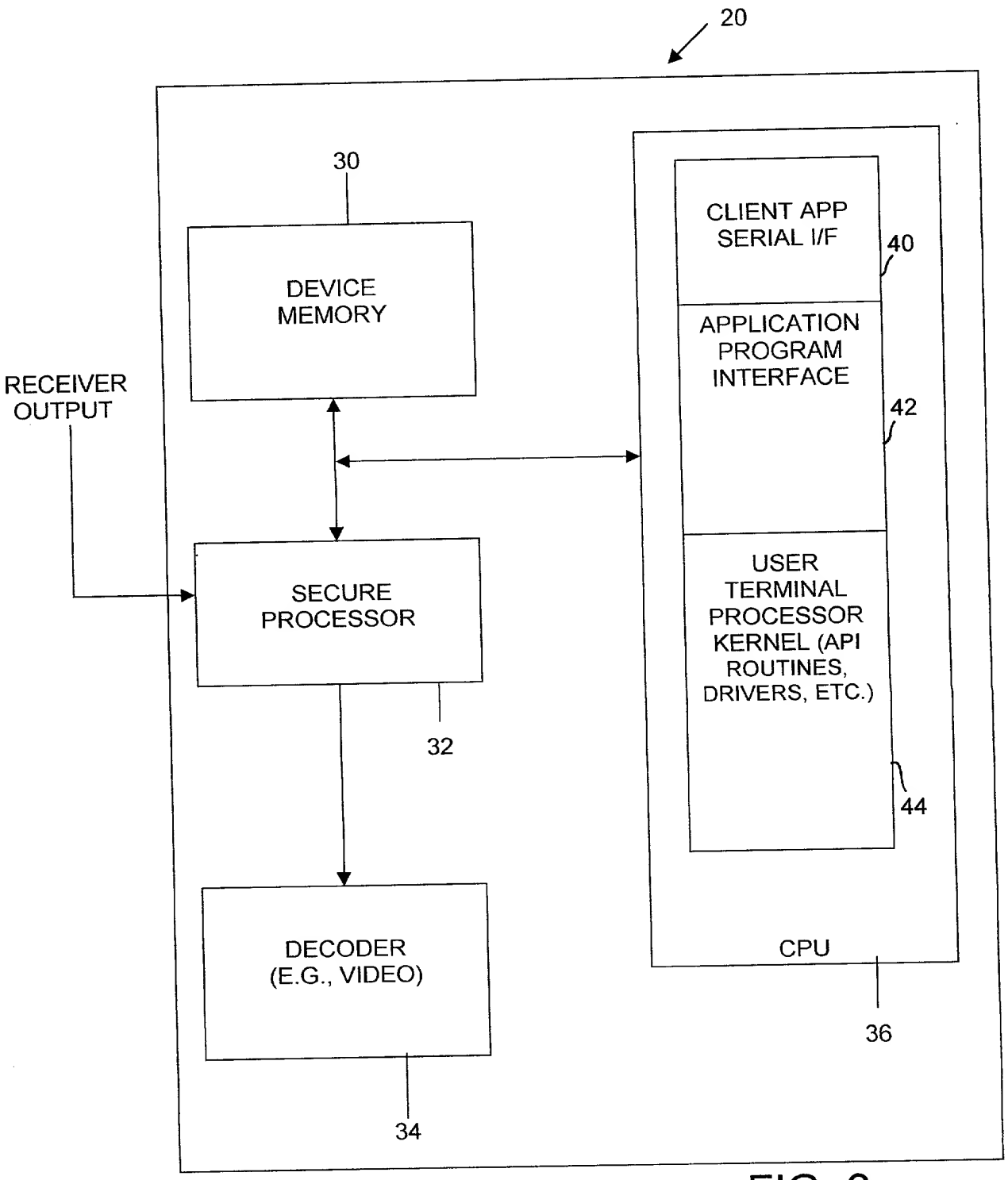
20
30
DEVICE MEMORY
RECEIVER OUTPUT
SECURE PROCESSOR
32
DECODER (E.G., VIDEO)
34
CLIENT APP SERIAL I/F
40
APPLICATION PROGRAM INTERFACE
42
USER TERMINAL PROCESSOR KERNEL (API ROUTINES, DRIVERS, ETC.)
44
CPU
36

FIG. 3

DECLARATION, POWER OF ATTORNEY, AND PETITION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES

the specification of which is attached hereto unless the following box is checked:

[X] was filed on **April 12, 2000** as PCT International Application Number **PCT/US00/09800** and was amended on **April 19, 2001** (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to be material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or of any PCT international application having a filing date before that of the application on which priority is claimed:

			Priority Claimed
(Number)	(Country)	Month/Day/Year Filed	[ ] Yes [ ] No
(Number)	(Country)	Month/Day/Year Filed	[ ] Yes [ ] No

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below.

60/132,366	**May 4, 1999**
(Application Number)	(Filing Date) - Month/Day/Year

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	**Parent Filing Date (MM/DD/YYYY)**	**Parent Patent Number (if applicable)**

And I hereby appoint: Barry R. Lipsitz, Registration No. 28,637 and Douglas M. McAllister, Registration No. 37,886, all of the firm of Barry R. Lipsitz, Attorney at Law, 755 Main Street, Bldg. 8, Monroe, Connecticut 06468, Telephone (203) 459-0200, my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Wherefore I pray that Letters Patent be granted to me for the invention or discovery described and claimed in the foregoing specification and claims, and I hereby subscribe my name to the foregoing specification and claims, declaration, power of attorney, and this petition.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor: **Reem Safadi**

Inventor's Signature Reem Safadi Date: 9/20/01

Residence **Horsham PA Pennsylvania** Citizenship: **U.S.A.**
(City) (State or Foreign Country)

Post Office Address **429 Brown Briar Circle Horsham Pennsylvania 19044, U.S.A.**
(Post Office Address) (City) (State & Zip Code/Country)

Full name of second joint inventor: **Lawrence D. Vince**

Inventor's Signature Lawrence D. Vince Date: 9/20/01

Residence **Lansdale PA Pennsylvania** Citizenship: **U.S.A.**
(City) (State or Foreign Country)

Post Office Address **114 Aileen Drive Lansdale Pennsylvania 19446, U.S.A.**
(Post Office Address) (City) (State & Zip Code/Country)